IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:		§		
		§		
	Ariel PELED et al.	§	Confirmation No.	9948
		§		
Serial No.:	10/815,764	§		
		§		
Filed:	April 2, 2004	§	Group Art Unit:	2166
		§		
For:	A METHOD AND A SYSTEM FOR INFORMATION IDENTIFICATION	§		
		§	Attorney Docket:	**27655**
Examiner:	Navneet K. AHLUWALIA	§		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313–1450

APPEAL BRIEF (37 C.F.R. 41.37)

Sir:

Further to the Notice of Appeal filed September 21, 2010, Appellant hereby files this Appeal Brief appealing the Examiner's Final Action of May 11, 2010 finally rejecting claims 1-25, 27-40, 49-59, 61 and 62.

This Appeal Brief is being filed on or before December 21, 2010, and for which a one month extension of time fee is due and enclosed herewith.

REAL PARTY IN INTEREST

The Real Party in interest is PortAuthority Technologies Inc., the assignee of record.

RELATED APPEALS AND INTERFERENCES

There are no Appeals, Interferences, or other judicial proceedings related to, directly affecting or affected by, or having a bearing on, the Board's decision in this Appeal.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN THE APPLICATION

The claims in the Application are: 1-25, 27-40, 49-59, 61 and 62.

B. STATUS OF ALL THE CLAIMS IN THE APPLICATION

Claims canceled: 26, 41-48 and 60.

Claims withdrawn from consideration but not canceled: NONE.

Claims pending: 1-25, 27-40, 49-59, 61 and 62.

Claims allowed: NONE.

Claims rejected: 1-25, 27-40, 49-59, 61 and 62.

Claims objected to: NONE.

C. CLAIMS ON APPEAL

The claims on appeal are: 1-25, 27-40, 49-59, 61 and 62.

STATUS OF AMENDMENTS

An Amendment after Final Rejection dated May 11, 2010 was not filed. Therefore, claims 1-25, 27-40, 49-59, 61 and 62 on appeal herein are as amended in the Response to Office Action filed on February 2, 2010.

SUMMARY OF CLAIMED SUBJECT MATTER

The appealed independent claims in the Application are claims 1 and 49, which are repeated below with reference to the specification by page and line number, and the drawings by the reference characters, in bold letters.

Independent **claim 1** defines a method for detecting distribution of an information item included within passing information sequences obtained from a digital medium, said information item comprising any one of a specified set of prestored information items whose distribution it is desired to control, comprising:

a) transforming each item of said set of prestored information items whose distribution it is desired to control from a first representation format into a respective format facilitating a first comparison, said first comparison being fast in relation to a second relatively slower textual comparison, in accordance with a predetermined transformation format, said predetermined transformation format being preservative of meaning; **{page 4, lines 12-13; page 15, lines 14-16}**

b) transforming passing information sequences, obtained from said digital medium, into said format facilitating said first relatively fast comparison in accordance with said transformation format; **{page 4, lines 14-15}**

c) determining the presence of one or more of said prestored information items within said transformed information sequence, said determining comprising: **{page 4, lines 16-18}**

comparing respective information sequences in said format facilitating said relatively fast comparison with said prestored information items in said format facilitating said relatively fast comparison; **{page 14, lines 13-14}**

d) when a match is found between said formats facilitating said relatively fast comparison then carrying out said second relatively slower textual comparison between said respective prestored information item in said first representation format and a respective information sequence obtained from said digital medium, and **{page 28, lines 10-11}**

e) when a match is found using said second relatively slower textual comparison, applying a policy to control distribution of said respective information sequence. **{page 7, lines 3-5}**

Independent **claim 49** defines an apparatus for detecting a predefined information item within a new information sequence for distribution control, said information item being any one of a specified set of data items, comprising:

a) a preprocessor, for transforming said predefined information item into a canonical representation said transformation being preservative of meaning, in accordance with a canonical transformation format; and {page 15, lines 6-9; element 120 in Fig. 1}

b) a scanner, for scanning said new information sequence to identify sub-sequences therewithin; and **{page 15, lines 21-22; element 150 in Fig. 1}**

c) a comparator associated with said preprocessor and said scanner, for making a first relatively fast comparison involving comparing said canonical representation to said identified sub-sequences to make an initial determination of the presence of said specified information item within said information sequence, and wherever a match is found using said relatively fast comparison involving canonical representation, then comparing original text of said sub-sequences and said specified information item to make a second determination of a match, the apparatus being configured to apply a policy for controlling distribution of said information sequence when said match is detected. **{page 15, line 23 to page 16, line 3; page 14, lines 13-14; page 28, lines 10-11; page 7, lines 3-5; element 160 in Fig. 1}**

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Final Action of May 11, 2010 included the following ground of rejection, which is now to be reviewed in this appeal:
Claims 1-25, 27-40, 49-59, 61 and 62 stand rejected under 35 U.S.C. §103(a) as being unpatentable over US Publ. 2003/0154399 to Zuk et al (herein "*Zuk*") in view of US Publ. 2005/0132070 to Redlich et al (herein "*Redlich*") further in view of US Publ. 2002/0107877 to Whiting (herein "*Whiting*").

Applicant believes that the US Publ. 2004/0068526 cited for *Redlich* in the OA of May 11, 2010 is incorrect. The correct *Redlich* reference number is understood to be US Publ. 2005/0132070, as listed in the Notice of References Cited in the final page of the Office Action dated August 18, 2009. This is supported by the Examiner's citation of *Redlich* paras. 0083 and 0089-0092, which paragraphs are not present in 2004/0068526 to Singh.

ARGUMENTS

A. GROUNDS OF REJECTION

Claims 1-25, 27-40, 49-59, 61 and 62 stand rejected under 35 U.S.C. §103(a) as being unpatentable over US Publ. 2003/0154399 to Zuk et al (herein "*Zuk*") in view of US Publ. 2004/0068526 to Redlich et al (herein "*Redlich*") further in view of US Publ. 2002/0107877 (herein "*Whiting*").

A.1 Claims 1 and 49 Distinguish over Cited References

Appellants respectfully submit that the Examiner has not provided a *prima facie* case of obviousness against independent claims 1 and 49. Specifically, the Examiner failed to show the following features of the claims in the cited references:

1) Transforming each item of said set of prestored information items whose distribution it is desired to control from a first representation format into a respective format facilitating a first comparison, said first comparison being fast in relation to a second relatively slower textual comparison, said predetermined transformation format being preservative of meaning (hereinafter "Feature (1)").

2) Transforming passing information sequences, obtained from said digital medium, into said format facilitating said first relatively fast comparison in accordance with said transformation format (hereinafter "Feature (2)"). Feature (2) corresponds to apparatus claim 51, which is dependent on independent claim 49.

3) Comparing information sequences in said format facilitating said relatively fast comparison with prestored information items in the same format. When a match is found, then carrying out said second relatively slower textual comparison between said respective prestored information item in said first representation format and a respective information sequence obtained from said digital medium (hereinafter "Feature (3)").

A.2 Feature (1) of Claims 1 and 49 Distinguishes over Cited References

Appellants respectfully submit that Feature (1) is missing in the cited references. If this feature is held as missing in the cited references, all of claims 1-25, 27-40, 49-59, 61 and 62 should be held allowable.

The Examiner states that Feature (1) is taught in *Zuk* paras. 4 and 9.

Zuk paras. 4 and 9 address a firewall function known as Network Address Translation (NAT). In para. 0009 *Zuk* describes NAT as:

> ...the source addresses of outgoing IP packets are rewritten to the IP address assigned to the firewall to give the impression that the packets originated from the firewall rather than from the internal hosts of the private network protected by the firewall. Reply packets coming back are translated and forwarded to the appropriate host.

However address translation is not preservative of meaning. In fact, a firewall is designed to ensure that the network address is not detectable by the recipient of the data packets. All meanings carried in the set of addresses is lost, as acknowledged by Zuk.

Furthermore, the process of NAT does not perform any transformation of the data carried by the data packets. NAT would fail to support the later stages of the claim where comparison is carried out, since in *Zuk* the information has been lost, making searching meaningless.

The Examiner does not allege that *Redlich* and *Whiting* teach the limitations of Feature (1) missing in *Zuk*.

Appellants therefore submit that *Zuk*, *Redlich* and *Whiting*, alone or in combination, fail to teach at least one feature of claims 1 and 49.

A.3 Feature (2) of Claims 1 and 49 Distinguishes over Cited References

Appellants respectfully submit that Feature (2) is missing in the cited references. If this feature is held as missing in the cited references, all of claims 1-25, 27-40, and 51 should be held allowable.

The Examiner cites *Zuk* paras. 0010 as teaching Feature (2). Applicants

respectfully believe that *Zuk* para. 0010 does not disclose transforming the information sequences into a format facilitating fast comparison.

Zuk para. 0010 does not teach any inventive feature whatsoever, but merely discusses the shortcomings of packet filtering firewalls. *Zuk* para. 0010 states:

> Packet filtering firewalls are relatively inexpensive and do not interfere with network performance, but alone they cannot typically provide adequate security. Packet filtering rules become unmanageable in complex environments, provide no user authentication mechanisms, and are vulnerable to attacks such as IP spoofing. For example, if a hacker can figure out a trusted IP address, the hacker may forge an IP header to a harmful packet. Being unable to differentiate between a valid packet and a forged one, a packet filtering firewall would not reject the harmful packet.

All the above passage teaches is that if a hacker can forge a trusted IP address a harmful packet may be undetectable by the firewall.

Applicants are at a loss to understand how *Zuk* para. 0010 describes any aspect of Feature (2). Specifically para. 0010 fails to teach "transforming passing information sequences, obtained from said digital medium, into said format facilitating said first relatively fast comparison in accordance with said transformation format" as claimed.

The Examiner does not allege that *Redlich* and *Whiting* teach the limitations of Feature (2) missing in *Zuk*.

Appellants therefore submit that *Zuk*, *Redlich* and *Whiting*, alone or in combination, fail to teach at least one feature of claims 1 and 51.

A.3 Feature (3) of Claims 1 and 49 Distinguishes over Cited References

Appellants respectfully submit that Feature (3) is missing in the cited references. If this feature is held missing in the cited references, all of claims 1-25, 27-40, 49-59, 61 and 62 should be held allowable.

The Examiner cites *Zuk* paras. 0024-0025 and *Whiting* paras. 0080-0081 as teaching Feature (3). In the Advisory Action of September 1, 2010 the Examiner further cites *Zuk* paras. 0100-0104.

The Examiner states that *Zuk* performs a first comparison in a first representation format and a secondary relatively slower textual comparison when a match is found. *Zuk* paragraphs 0024-0025 teach that firewalls, which perform NAT, are not capable of detecting and stopping network attacks, and that Intrusion Detection Systems provide a second level of security by analyzing collected information for signs of intrusion.

Neither address translation nor information collection and analysis constitute determining the presence of one or more prestored information items within a transformed information sequence, as required by the claim. There is certainly no teaching that there are two searches which are in any way connected, such as by one being faster than the other or by one depending on the results of the other. In fact, *Zuk* paragraph 0025 specifically states that intrusion information system could be placed first or second.

The Examiner further cites *Zuk* paras. 0100-0104 as disclosing the claimed two-stage comparison. The Examiner states that in *Zuk* a first detection of information serves as a first faster search, followed by a detailed comparison.

Zuk paras. 0100-0104 describe two separate functions:

1) Function 1 - Determining whether the incoming packets are compliant with the protocol used to transmit them and whether the actions or commands embodied in the packets or data streams are authorized or allowed for the protocol. (see *Zuk* paras. 0100-0101).

2) Function 2 - Matching known attack signatures to the packet headers and data according to the network protocol used to transmit the packet (see *Zuk* paras. 0102-0103).

In contrast with the claimed herein, *Zuk* does not perform two searches between prestored information sequences and passing information sequences. In *Zuk*, the two functions constitute separate searches of different portions of the data packets or stream. Function 1 serves as a filter for dropping data packets with suspect protocols. Only those packets which are not dropped are searched for attack signatures by Function 2. This is directly opposed to the claimed embodiments, in which the first search serves to identify information sequences which should undergo the slower textual search.

Furthermore, there is no indication that *Zuk*'s Function 2 involves any type of textual search. *Zuk* specifically states that the attack signature may be searched for in both the packet header and data. There is no indication that any portion of either the header or the data are textual, or that the signature being searched for is of a textual nature.

The Examiner further cites *Whiting* paras. 0080-0081 as teaching the fast comparison of formatted files and slower comparison if a match is found.

Whiting paras. 0080-0081 do present searching at two levels. However neither search is performed on the complete content, contrary to the requirement of the claim. As discussed in *Whiting* paragraph 77, the first level is a *subset* of bits of the material in the file to be compared, which bits are *randomly selected*. The second level comprises the remaining bits not included in the first level. Random selection of bits does not constitute a "format for rapid search", since performing the random selection twice on the same content will not yield the same results.

Furthermore, in contrast with the claims herein, neither *Whiting* search comprises a textual search. Both searches in *Whiting* are bit-level searches, not textual searches. The second Whiting search, of a level made up of remaining bits, is not eligible for a full textual search. Indeed there is no requirement in *Whiting* that the files are text at all.

Appellants therefore submit that *Zuk*, *Redlich* and *Whiting*, alone or in combination, fail to teach at least one feature of claims 1 and 49.

A.4 No Basis for Combining References

The Examiner failed to provide a *prima facie* case of obviousness against claims 1-25, 27-40, 49-59, 61 and 62, since the Final Office Action of May 11, 2010 did not state a proper reason to combine the *Zuk, Whiting* and *Redlich* references.

For motivation to combine the references the Examiner states that the cited references are in the same field of invention, that of information storage and identification. The Examiner further states that the combination with *Whiting* improves the speed of execution and matches since unnecessary data is not searched very

thoroughly.

Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'" *KSR International Co. v. Teleflex Inc. (KSR), 82 USPQ2d 1385 (2007).*

Applicant respectfully assert that a person skilled in the art would not be motivated to combine *Zuk*, *Redlich* and *Whiting*. The Examiner cites *Zuk*'s address translation as comprising a transforming of prestored information items into a format facilitating a fast comparison. It is these transformed information items which serve as one of the inputs to the comparison.

Appellants submit that a person of ordinary skill in the art would be lead against such combination. Address translation transforms all originating data addresses to a single firewall address. Indeed the goal of address translation is that no search for the original addresses will yield useful results. Therefore performing *Whiting*'s bit search on the prestored information items transformed by address translation will return a uniform result for all searches. Since a search is futile in *Zuk*, the skilled person has no motivation to look at *Whiting* to find a two-level search to improve the speed of the futile search.

Conclusion

Claims 1-25, 27-40, 49-59, 61 and 62 are believed to patentably distinguish over *Zuk*, *Redlich* and *Whiting*, in any combination, for at least all of the above reasons. Therefore, it is respectfully requested that the Board reverse the Examiner's Final Rejection for those claims.

Appellants are separately arguing the patentability of independent claims 1 and 49 and of dependent claim 51. The other pending claims are patentable at least by virtue of their dependency on a patentable parent claim.

Respectfully submitted,

/Jason H. Rosenblum/

Jason H. Rosenblum
Registration No. 56,437
Telephone: 718.246.8482

Date: December 16, 2010

CLAIMS APPENDIX

The claims now pending in the application are as follows:

1. A method for detecting distribution of an information item included within passing information sequences obtained from a digital medium, said information item comprising any one of a specified set of prestored information items whose distribution it is desired to control, comprising:

transforming each item of said set of prestored information items whose distribution it is desired to control from a first representation format into a respective format facilitating a first comparison, said first comparison being fast in relation to a second relatively slower textual comparison, in accordance with a predetermined transformation format, said predetermined transformation format being preservative of meaning;

transforming passing information sequences, obtained from said digital medium, into said format facilitating said first relatively fast comparison in accordance with said transformation format;

determining the presence of one or more of said prestored information items within said transformed information sequence, said determining comprising:

comparing respective information sequences in said format facilitating said relatively fast comparison with said prestored information items in said format facilitating said relatively fast comparison;

when a match is found between said formats facilitating said relatively fast comparison then carrying out said second relatively slower textual comparison between said respective prestored information item in said first representation format and a respective information sequence obtained from said digital medium, and

when a match is found using said second relatively slower textual comparison, applying a policy to control distribution of said respective information sequence.

2. A method according to claim 1, further comprising storing said representations in a database.

3. A method according to claim 1, further comprising sorting said representations into a sorted list.

4. A method according to claim 3, wherein said sorting is in accordance with a tree sorting algorithm.

5. A method according to claim 1, wherein said information item comprises a single word.

6. A method according to claim 1, wherein said information item comprises a sequence of words.

7. A method according to claim 1, wherein said information item comprises a delimited sequence of sub-items.

8. A method according to claim 7, wherein each of said sub-items comprises a sequence of alphanumeric characters.

9. A method according to claim 1, wherein a type of said information item comprises one of a group of types comprising: a word, a phrase, a number, a credit-card number, a social security number, a name, an address, an email address, and an account number.

10. A method according to claim 1, wherein said information sequence is provided over a digital traffic channel.

11. A method according to claim 10, wherein said digital traffic channel comprises one of a group of channels comprising: email, instant messaging, peer-to-peer network, fax, and a local area network.

12. A method according to claim 1, wherein said information sequence comprises the body of an email.

13. A method according to claim 1, wherein said information sequence comprises an email attachment.

14. A method according to claim 1, further comprising retrieving said information sequence from a digital storage medium.

15. A method according to claim 14, wherein said digital storage medium comprises a digital cache memory.

16. A method according to claim 1, wherein said representation depends only on the textual and numeric content of the information item.

17. A method according to claim 1, wherein said transforming into a format that facilitates fast comparison comprises Unicode encoding.

18. A method according to claim 1, wherein said transforming into a format that facilitates fast comparison comprises converting all characters to upper-case characters or to lower-case characters.

19. A method according to claim 1, wherein said transforming into a format that facilitates fast comparison comprises encoding an information item into a numeric representation.

20. A method according to claim 1, wherein said transforming into a format that facilitates fast comparison comprises applying a first hashing function to said representations.

21. A method according to claim 1, wherein said information sequence comprises sub-sequences.

22. A method according to claim 21, wherein said sub-sequences are separated by delimiters.

23. A method according to claim 22 wherein said sub-sequences separated by delimiters are any of: words; names, and numbers.

24. A method according to claim 23, further comprising scanning said information sequence to identify said sub-sequences.

25. A method according to claim 24, and said determining is performed by matching said information item to an ordered series of said sub-sequences.

27. A method according to claim 1, wherein said policy is a security policy, said security policy comprises at least one of the following group of security policies: blocking said transmission, logging a record of said detection and detection details, and reporting said detection and detection details.

28. A method according to claim 27, wherein said information items are divided into sets, and wherein said security policy depends on the number of detected information items that belong to the same set.

29. A method according to claim 28 wherein each of said sets comprises information items associated with a single individual.

30. A method according to claim 1, wherein said information item comprises a sequence of sub-items.

31. A method according to claim 30, wherein said sub-items are separated by delimiters.

32. A method according to claim 30, wherein a sub-item comprises one of a group comprising: a word, a number, and a character string.

33. A method according to claim 30, wherein said determining comprises using a state machine operable to detect said sequence of delimited sub-items within said information sequence.

34. A method according to claim 30, wherein said transforming into a format facilitating fast comparison comprises:

applying a first hashing function to assign a respective preliminary hash value to each sub-item within said information item; and

applying a second hashing function to assigning a global hash value to said information item based on said preliminary hash values of said sub-items.

35. A method according to claim 34, wherein said information sequence comprises sub-sequences, and wherein said determining comprises:

applying said first hashing function to assign a respective preliminary hash value to each of said sub-sequences;

applying said second hashing function to at least one of said preliminary hash values to assign a global hash value to said at least one of said sub-sequences; and

comparing said global hash value to hash values of said sub-sequences.

36. A method according to claim 35, wherein said sub-sequences comprise one of a group comprising: a word, a number, and a character string

37. A method according to claim 35, wherein said sub-sequences comprise a plurality of ordered combinations of sub-sequences within said data sequence.

38. A method according to claim 36, wherein said sub-sequences comprise a plurality of combinations of sub-sequences within said data sequence.

39. A method according to claim 38, wherein said second hash function is invariant to reordering of at least two of said sub-sequences.

40. A method according to claim 39, further comprising checking whether a delimited segment was previously stored, and continuing said detection process only if a current delimited segment was previously stored.

49. An apparatus for detecting a predefined information item within a new information sequence for distribution control, said information item being any one of a specified set of data items, comprising:

a preprocessor, for transforming said predefined information item into a canonical representation said transformation being preservative of meaning, in accordance with a canonical transformation format; and

a scanner, for scanning said new information sequence to identify sub-sequences therewithin; and

a comparator associated with said preprocessor and said scanner, for making a first relatively fast comparison involving comparing said canonical representation to said identified sub-sequences to make an initial determination of the presence of said specified information item within said information sequence, and wherever a match is found using said relatively fast comparison involving canonical representation, then comparing original text of said sub-sequences and said specified information item to make a second determination of a match, the apparatus being configured to apply a policy for controlling distribution of said information sequence when said match is detected.

50. An apparatus for detecting a specified information item within an information sequence according to claim 49, further comprising a user interface for inputting said information items.

51. An apparatus for detecting a specified information item within an information sequence according to claim 49, wherein said scanner is further operable to transform said information sequence in accordance with said canonical transformation format.

52. An apparatus for detecting a specified information item within an information sequence according to claim 49, wherein said scanner is further operable to transform said sub-sequences in accordance with said canonical transformation format.

53. An apparatus for detecting a specified information item within an information sequence according to claim 49, further comprising a database for storing a representation of each data item of said set.

54. An apparatus for detecting a specified information item within an information sequence according to claim 49, wherein said information sequence is obtained from a digital medium.

55. An apparatus for detecting a specified information item within an information sequence according to claim 49, further comprising a sorter, for forming a sorted list of the respective representations of set of data items.

56. An apparatus for detecting a specified information item within an information sequence according to claim 49, wherein a type of said information item comprises one of a group of types comprising: a word, a phrase, a number, a credit-card number, a social security number, a name, an address, an email address, and an account number.

57. An apparatus for detecting a specified information item within an information sequence according to claim 49, wherein said information sequence is provided over a digital traffic channel.

58. An apparatus for detecting a specified information item within an information sequence according to claim 49, further comprising retrieving said information sequence from a digital storage medium.

59. An apparatus for detecting a specified information item within an information sequence according to claim 58, wherein said digital storage medium comprises digital storage medium within a proxy server.

61. An apparatus for detecting a specified information item within an information sequence according to claim 49, wherein said encoding function comprises a hashing function.

62. A method according to claim 2, wherein said transforming said representation and storage of said information items comprises:

a) assigning a hash value to each delimited segment within said information item;

b) assigning a hash value for said information item based on said hashes assigned to delimited segments within said information item;

c) storing said hash values evaluated in step a) and step b) above;

and wherein detecting said information items within said digital medium comprises:

d) assigning a hash value to each delimited segment within said digital medium utilizing the same hash function used in step a) above;

e) assigning a hash value for sequences of delimited segments utilizing the same hash function used in step b) above, said sequences being of pluralities of possible numbers of delimited segments within said information items;

f) comparing the hashes values evaluated in step e) above with said hash values stored in step e) above.

EVIDENCE APPENDIX

This appeal has no evidence appendices.

RELATED PROCEEDINGS APPENDIX

This appeal has no related proceedings.